Health Insurance Portability and Accountability Act of 1996 (HIPPA)

The Privacy Rule

- (2003; 45 CFR Parts 160 and 164) of the Health Insurance Portability and Accountability Act (HIPAA)
- Created a category of health information, referred to as "protected health information" (PHI), which is a subset of "individually identifiable health information" that may be used or disclosed to others.
- Applies to covered entities

Who are covered entities?

- Covered entities include health plans, health care clearinghouses, and health care providers that transmit health information electronically in connection with certain defined HIPPA transactions, such as claims or eligibility inquiries.
- Researchers themselves are NOT covered entities, unless they are also health care providers and engage in any of the covered electronic transactions.
    - However, if researchers are employees or other workforce members of a covered entity, they may have to comply with that entity's Privacy Rule policies and procedures.
    - Researchers who are not covered entities, or who are not workforce members of covered entities, may be indirectly affected by the Privacy Rule if covered entities supply their data.

Disclosure of PHI

The Privacy Rule permits covered entities to use or disclose "protected health information" (PHI) for research purposes either with an individual's specific written permission, termed "Authorization," or without it, if certain conditions are met.

- Obtain the individual's Authorization for the research use or disclosure of PHI,
- Obtain satisfactory documentation of an Institutional Review Board (IRB) or Privacy Board' s waiver of the Authorization requirement,
- Obtain satisfactory documentation of an IRB or Privacy Board's alteration of the Authorization requirement as well as the altered Authorization from the individual,
- Use or disclose PHI for research solely on decedents' PHI with representations from the researcher that satisfy the Privacy Rule,
- Provide a limited data set and enter into a data use agreement with the recipient,
- USE OR DISCLOSE INFORMATION THAT IS DE-IDENTIFIED in accordance with the standards set by the Privacy Rule (**in which case, the health information is not longer PHI**), or
- Use or disclose PHI based on permission that predates the applicable compliance date of the Privacy Rule.

De-Identified Data Sets

The Privacy Rule permits covered entities to use and disclose data that have been de-identified without obtaining Authorization and without further restrictions on use or disclosure because de-identified data are not PHI and, therefore, are not subject to the Privacy Rule.

There are two ways of de-identifying data: the "safe-harbor" method and statistically.

- The safe-harbor method - requires the removal of every one of the 18 identifiers; data that are stripped of these 18 identifiers are regarded as de-identified, unless the covered entity has actual knowledge that it would be possible to use the remaining information alone or in combination with other information to identify the subject.
- Statistically - have a qualified statistician determine, using generally accepted statistical and scientific principles and methods, that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by the anticipated recipient to identify the subject of the information.
    - A statistician is defined as a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable.
    - The qualified statistician must document the methods and results of the analysis that justify such a determination.

Re-identification of Data

The Privacy Rule permits a covered entity to assign to, and retain with, the de-identified health information a code or other means of record re-identification, if the following conditions are met.

- First, the re-identification code may not be derived from or related to information about the individual or otherwise be capable of being translated to identify the individual.
- Second, the covered entity may not use or disclose the code for any other purpose or disclose the mechanism for re-identification.

F.A.Q.s

- May a covered entity hire a researcher as a business associate to de-identify health information when the researcher is the intended recipient of the de-identified data?
    - Yes. A covered entity may hire the intended recipient of the de-identified data as a business associate for purposes of creating the de-identified data. However, the data recipient, as a business associate, must agree to return or destroy the identifiers once the de-identified data set has been created.
- May a covered entity that has hired a researcher as its business associate for the purposes of de-identifying data permit the researcher to assign to the de-

identified data a re-identification code, if the researcher is also the intended recipient of the de-identified data?

- Yes, provided the researcher is able to return or destroy all identifiers once the de-identified data set has been created, as required by his or her business associate contract. This would include the researcher's providing to the covered entity the mechanism for re-identification and retaining no copy or other method of re-identification.
- In cases where the researcher has a standard method for assigning a re-identification code that necessarily remains with the researcher even after the other identifiers have been returned or destroyed, the information is not considered de-identified if the researcher assigns such as re-identification code.